Claims:

1. (Cancelled).

2. (Currently amended) A method for securely transmitting transaction data over a network having at least a public component, the transaction data including account PIN data and non-PIN data, the method comprising:

performing a first encryption operation only on the PIN data; and

performing a second encryption operation on at least the non-PIN data, such that the PIN data is cryptographically isolated from the non-PIN data; and

transmitting the cryptographically isolated PIN data and non-PIN data over the network to a remote location having only the capability to decode the second encryption operation, wherein ~~The method of encoding transaction data of claim 1, wherein:~~ said first encryption operation uses an asymmetrical encryption process and said second encryption operation uses a symmetrical encryption process.

3. (Currently Amended) The method of encoding transaction data of ~~claim 2~~ claim 1, wherein said symmetrical encryption process uses a secret encryption key and wherein said method includes the further step of performing a third encryption operation on said secret encryption key.

4. (Currently Amended) The method of encoding transaction data of ~~claim 1~~ claim 2, wherein said second encryption process is performed on both the PIN and non-PIN data, such that the encrypted PIN data resides within an encrypted envelope generated by the second encryption operation.

5. (Currently Amended) The method of encoding transaction data of ~~claim 1~~ claim 2, further comprising the steps of:

calculating a digest by applying a one-way mathematical process to the non-PIN data; and

appending the digest to the PIN data blocks for future verification of the non-PIN data.

6. (Cancelled)

7. (Currently Amended) A method for decoding encrypted transaction data, the transaction data including account PIN data input by a user as well as non-PIN data, comprising the steps:

receiving the encrypted transaction data from a first remote location over a network having at least a public component;

performing at the first remote location, a first decryption operation to decode only the encrypted non-PIN data;

transmitting at least the encrypted account PIN data to a second remote location; and

performing at the second remote location a second decryption operation to decode the encrypted account PIN data, wherein said second decryption operation is different from the first decryption operation, wherein ~~The method of decoding encrypted transaction data of claim 6, wherein:~~ said first decryption operation uses a symmetrical decryption process and said second decryption operation uses an asymmetrical decryption process.

8. (Currently amended) The method of decoding encrypted transaction data of ~~claim 6~~ claim 7, further comprising the steps:

calculating a digest by applying a one-way mathematical process to the non-PIN data; and

comparing the calculated digest to a received digest formed with the same one-way mathematical process and appended to the PIN data blocks for verifying the non-PIN data.

9 - 16. (canceled)

17. (Currently Amended) A method of transporting PIN data input by a user and non-PIN data in a secure electronic transfer, comprising the steps:

encrypting only the PIN data using a first encryption process,

encrypting at least the non-PIN data using a second encryption process;

transmitting the encrypted PIN and non-PIN data over a data network to an authentication requestor at a remote location, said authentication requestor having means to decrypt only the non-PIN data;

transmitting the encrypted PIN data over a data network to an authorizing agent for verification;

decrypting and verifying the PIN data by the authorizing agent; and

transmitting a notification over a data network, from the authorizing agent to the authentication requestor, of a verification status of the PIN data,

wherein ~~The method of transporting PIN and non-PIN data of claim 16, wherein:~~ said first encryption process is an asymmetrical encryption process and said second encryption process is a symmetrical encryption process.

18. (Previously presented) The method of transporting PIN and non-PIN data of claim 17, wherein the asymmetrical encryption process is performed using a public key provided to an account holder by the authorizing agent and wherein said decrypting performed by the authorizing agent is performed using a private key associated with the public key.

19. (Previously presented) The method of transporting PIN and non-PIN data of claim 18, wherein said symmetrical encryption process uses a secret encryption key and wherein said method includes the further step of performing a third encryption operation on said secret encryption key.

20. (Currently amended) The method of transporting PIN and non-PIN data of ~~claim 16~~ claim 17, further comprising the steps of:

prior to transmitting the encrypted PIN and non-PIN data, calculating a first digest by applying a one-way mathematical process to the non-PIN data and appending the digest to the PIN data blocks; and

after transmitting the encrypted PIN and non-PIN data, calculating a second digest by applying the same one-way mathematical process to the non-PIN data and comparing the first digest and second digest to verify the non-PIN data.

21. (Cancelled)

22. (Currently Amended) A terminal for encoding transaction data including account PIN data input by a user as well as non-PIN data, comprising:

means for performing a first encryption operation only on the PIN data; and

means for performing a second encryption operation on at least the non-PIN data, such that the PIN data is cryptographically isolated from the non-PIN data; ~~and~~

means for transmitting the cryptographically isolated PIN data and non-PIN data over a data network to a remote location;

transmitting the cryptographically isolated PIN data and non-PIN data over the network to a remote location having only the capability to decode the second encryption operation, wherein ~~The terminal for encoding transaction data of claim 21, wherein:~~ said first encryption means uses an asymmetrical encryption process and said second encryption means uses a symmetrical encryption process.

23. (Currently Amended) The terminal for encoding transaction data of ~~claim 21~~ claim 22, further comprising a card reader for acquiring at least a portion of the transaction data from a payment instrument.

24. (Cancelled)

25. (Currently amended) A system for decoding encrypted transaction data including account PIN data input by a user as well as non-PIN data, comprising:

means for receiving the encrypted transaction data from a remote location;

means for performing a first decryption operation to decode the encrypted non-PIN data; and

means for transmitting at least the encrypted account PIN data to a second remote location; and

means for performing at the second remote location a second decryption operation to decode the encrypted account PIN data, wherein said second decryption operation is

different from the first decryption operation, wherein ~~The system as defined by claim 24, wherein:~~ said first decryption means uses a symmetrical decryption process and said second decryption means uses an asymmetrical decryption process.

26. (Cancelled)

27. (Cancelled)

28. (Currently Amended) A system for encoding and transporting PIN data input by a user and non-PIN data comprising:

first means for encrypting only the PIN data using a first encryption process;

second means for encrypting at least the non-PIN data using a second encryption process;

means for transmitting the encrypted PIN and non-PIN data over a data network to an authentication requestor, said authentication requestor having means to decrypt only the non-PIN data;

means for transmitting the encrypted PIN data over a data network to an authorizing agent for verification;

means for decrypting and verifying the PIN data by the authorizing agent; and

means for notifying the authentication requestor over a data network of a verification status of the PIN data, wherein ~~The system for encoding and transporting PIN and non-PIN data of claim 27, wherein:~~

said first encryption means employs an asymmetrical encryption process~~;~~ and , wherein

said second encryption means employs a symmetrical encryption process.

29. (Currently amended) The system for encoding and transporting PIN and non-PIN data of ~~claim 27~~ claim 28, wherein the first encryption means uses a public key provided to an account holder by the authorizing agent and wherein said decrypting means uses a private key associated with the public key.

30. (Previously presented) The system for encoding and transporting PIN and non-PIN data of ~~claim 27~~ claim 28, further comprising:

means for calculating a first digest by applying a one-way mathematical process to the non-PIN data and appending the digest to the PIN data blocks prior to transmitting the encrypted PIN and non-PIN data; and

means for calculating a second digest by applying the same one-way mathematical process to the non-PIN data and comparing the first digest and second digest after transmitting the encrypted PIN and non-PIN data, to verify the non-PIN data.

31. (Previously presented) The system for encoding and transporting PIN and non-PIN data of ~~claim 24~~ claim 28, further comprising a card reader for acquiring at least a portion of the PIN and non-PIN data from a payment instrument.

32. - 36 (Cancelled)

37. (Currently amended) A method for decoding encrypted transaction data, the transaction data including encrypted account PIN data encrypted by a first encryption operation as well as encrypted non-PIN data encrypted with a second, different encryption operation, comprising the steps:

receiving the transaction data from a remote location over a network having at least a public component, wherein said remote location does not have the capability to decode the encrypted PIN data;

performing a first decryption operation to decode the encrypted non-PIN data; and

transmitting at least said encrypted PIN data to another remote location for a second decryption operation, wherein ~~The method of decoding encrypted transaction data of claim 35, wherein~~: said first decryption operation uses a symmetrical decryption process and said second decryption operation uses an asymmetrical decryption process.

38. (Cancelled)

39. (Cancelled).